REMARKS

Claims 1-8, 10-17, 21-25, and 36-38 are pending. The claims are rejected in view of new grounds under Section 102(e). The Office Action now cites a new reference, Taylor, as the basis for rejection, no longer citing the Toubul reference.

Claims 1 and 16 have been amended to further specify that if the request for content does not have a protocol that is only for requesting and retrieving content, then the request is not altered in any way (a redirection destination header is not added) and it is not sent to a proxy server. These amendments are made to address the §112 issues raised in the Office Action.

The Taylor reference discloses a Dynamic Packet Filter (DFP) in a firewall. The DFP has numerous filtering rules, some of which are "user specified static filter rules" which include certain types of filters, one of which is "absorb" which applies application level filters. In order to provide finer granularity in the packet filtering, the packet filter is extended to include additional fields such as TCP flags.

These filter rules are cited as disclosing the scan module of the claimed invention. As recited in the claims, the scan module identifies the request as a request for content by scanning a protocol field and identifying a protocol that is only for requesting and retrieving content. The claim also recites a proxy module that modifies the request if the protocol is one only for requesting and retrieving content. This specific type of filtering as recited in the claims is not disclosed or taught in Taylor. None of the filters described in Taylor disclose the recited filtering done by the scan module before the request is processed for transmission to the target server and by specifically scanning the protocol field of the request.

The Taylor reference is also cited as anticipating the proxy server component (claim 1) and step (claim 16) of the claimed invention. The Taylor reference discloses a transparency procedure for the firewall. FIG. 7 of Taylor shows examples of procedures for transparency where if transparency is OFF, the source address is modified to reflect the IP address of firewall and the packet is forwarded to the external host. When the external host sends an acknowledging packet, the address is of the firewall and not the internal host that sent the packet. In this manner, there is no transparency to the external host as to which component behind the firewall is sending the packet. Although the address of the packet may be changed depending on whether transparency is ON or OFF, the reference does not disclose or anticipate the claimed invention, specifically the proxy server having a decoding module for decoding the response from the target server, a content scanning module to scan the decoded response and a user-defined configuration data scanning module to apply user-defined configuration data to the decoded response. These various features, all of which are specifically recited in the claims, are not disclosed or taught by the transparency example shown in Taylor.

As provided in the previous response, the request is scanned and if a protocol field in the request indicates that the request is solely intended to request and retrieve content (a "request/retrieve" protocol as described on page 13 of the specification), the request is modified by a proxy module so that it is redirected to a proxy server. The claims recite that the protocol field of the request is scanned in a redirection program before the request is transmitted on the network. In other words, the request is examined immediately upon being sent by a user. These features are not shown or taught in Taylor.

For these reasons, Applicant believes the amended claims and the dependent claims are patentable over the cited references.

Respectfully submitted,
BEYER LAW GROUP LLP

/Rupak Nag/

Rupak Nag
Registration No. 37,493

BEYER LAW GROUP LLP
P.O. Box 1687
Cupertino, CA 95014-1687
Telephone: (612) 252-3335
Fax No.: (612) 825-6304